Data Protection Policy

Business Area: Data Protection Office

Version: 11.0

Document Reference: POL-18-060

Document Control

Status: Live

Document Version History (last 4 versions)

Date	Version	Author	Comments
03/07/2020	8.0		Annual Review
12/07/2021	9.0		Annual Review plus Risk Appetite Alignment section added
20/09/2023	10.0		Biennial Review
05/08/2025	11.0		Biennial Review

Review and Approval Register

Note: RACI = R- Responsible, A- Accountable, C-Consulted, I-Informed

Name	Position	RACI Role
Gary Womersley	Data Protection Officer ("DPO")	**A**
	Information Assurance and Governance Senior Manager/Deputy DPO	**R**
	Chief Information Security Officer	**I**
	Information Assurance Governance Officer (Data Protection)	**C**
	Information Assurance Governance Analyst – Data Protection	**C**
	Senior Manager – Legal	**C**
	Legal Services	**C**
	Risk Director	**C**

***NB: names of staff other than DPO have been removed under section 40(2) of the Freedom of Information Act 2000**

Update Schedule

The Data Protection Policy (the "Policy") is reviewed on an as needs basis, but no less than once in any rolling 24-month period and may be amended at any time. The Data Protection Office ("DP Office") will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives. Recommendations for any amendments should be emailed to the DP Office (please refer to section 8 below for contact details).

Applicability

The requirements in this Policy apply to all permanent, temporary and contract workers employed or engaged by Student Loans Company Limited ("SLC") (collectively hereinafter referred to as an "employee") and to any 3rd party organisations while working or engaged on SLC business.

Compliance

Any employee found to have violated this Policy could be subject to disciplinary action, up to and including termination of their employment.

At its sole discretion, SLC may require the removal from the service provision account of any employee of a 3rd party organisation contractually engaged on SLC business, who has been evidenced to have violated this Policy.

Contents

1 Overview

1.1 Introduction

1.1.1 Student Loans Company Limited ("SLC", "we", "us" and "our") is a non-profit making Government owned organisation set up to provide loans and grants to students in universities and colleges in the United Kingdom ("UK").

1.1.2 The UK General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018 (collectively referred to as "Data Protection Legislation"), regulate the processing of personal data and protect the rights of the data subject.

1.1.3 As SLC processes personal data, we are registered as a data controller (Registration Number Z7261665) with the Information Commissioner's Office ("ICO"). This means we are responsible for deciding how we hold and use personal data. In certain circumstances, we may act as a joint data controller (please refer to section 2.5 Purposes of Processing, which refers to SLC's Privacy Notices for more detail).

1.1.4 Data Protection Legislation governs how we obtain, handle, store, destroy and process personal data.

1.2 Scope

1.2.1 This Policy applies to all data subjects in relation to whom SLC holds personal data, whether received directly or indirectly, in order to carry out SLC functions.

1.3 Risk Appetite Alignment

1.3.1 The requirements of this Policy support the mitigation of risks within the Security risk category outlined in the SLC risk language.

1.3.2 Compliance with Policy requirements ensures that SLC continues to operate within its risk appetite, which is:

- Cautious appetite towards Security risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with Data Protection Act 2018 requirements.

1.3.3 A number of scenarios where a more granular risk tolerance applies are defined in the Security and Information Risk Appetite Statement, representing a greater or lesser appetite for risks posed by a specific system, process or asset.

1.4 Status of Policy

1.4.1 This Policy sets out SLC's rules on data protection and the legal conditions that must be satisfied regarding the obtaining, handling, processing, storage, and destruction of personal data.

1.4.2 SLC's designated Data Protection Officer ("DPO") is responsible for monitoring compliance with Data Protection Legislation and this Policy. Any questions or concerns about the operation

of this Policy should be referred in the first instance to the DP Office (please refer to section 9 below for contact details).

1.4.3 If you consider this Policy has not been complied with, then you should raise the matter with SLC's DP Office at DPO@slc.co.uk.

2 Data Protection Legislation

2.1 Background

2.1.1 Data Protection Legislation regulates the processing of personal data in order to protect the interests of the data subject.

2.1.2 Data Protection Legislation covers a wide range of matters, scenarios, and issues. These can be specific and as a result, you may find that certain aspects of data protection guidance are set out in more detail in separate SLC policies and guidelines. When relevant, these have been referenced within this Policy.

2.2 Definitions

2.2.1 There are a number of key definitions used within Data Protection Legislation that are essential to understanding this Policy and SLC's obligations under Data Protection Legislation.

- **"data"** – means information held electronically (eg. computers, personal organisers, laptops), manually or in paper form as part of a filing system.
- A **" filing system"** means any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- **"personal data"** – means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data include name, telephone number, age, qualifications and employment history.
- **"data controller"** – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **"data processor"** – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **"data protection officer"** - the individual whose primary role is to ensure that their organisation processes the personal data of its employees, customers, providers or any other data subjects in compliance with the applicable Data Protection Legislation.
- **"data subject"** – means an identified or identifiable natural person. Data subjects may include employees, contractors, customers, job applicants, candidates and suppliers; and the data processed may relate to present, past and prospective data subjects.

- **"processing"** – means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Process" and "processed" will be construed accordingly.
- **"special category data**" – means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.3 Data Protection Principles

2.3.1 SLC has a duty to ensure that all personal data (however collected) is processed in accordance with the below principles, as detailed in Data Protection Legislation.

2.3.2 Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, be kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.4 Special Category, Criminal Convictions Data and SLC Sensitive Information

2.4.1 SLC employees may in certain circumstances become privy to special category and criminal convictions data.

2.4.2 Data Protection Legislation states that special category data should only be collected, processed, or disclosed in very specific circumstances, such as if explicit consent has been provided, as it is recognised that the processing of this data may create significant risks to the data subject's rights and freedoms.

2.4.3 Criminal record data is not special category data; however, it is protected under Data Protection Legislation.

2.4.4 Sensitive Information - SLC may also store and process sensitive information which, while not meeting the definition of special category data, is deemed sensitive and therefore requires additional handling arrangements. For example, bank and financial details and interview transcripts.

2.5 Purposes of Processing

2.5.1 Please see the applicable Privacy Notice for information in relation to the purpose for which personal data is processed.

Customer Privacy Notice
Applicant Privacy Policy

2.6 Data Retention

2.6.1 Please see the Records Management Policy for more detail in relation to the period for which personal data is retained.

2.7 Rights of the Data Subject

2.7.1 Data Protection Legislation establishes rights for data subjects regarding the processing of their personal data ie. their right to:

- be informed about the collection and use of their personal data (Right to be informed);
- obtain access to their personal data (please refer to section 5 for more detail) (Right of access);
- request to have certain personal data corrected, or completed if it is incomplete (Right to rectification);
- have personal data erased (Right to erasure);
- request certain personal data is restricted from processing. This enables the data subject to ask us to suspend the processing of personal data about the data subject, where for example the data subject wants us to establish its accuracy or the reason for processing (Right to restrict processing);
- data portability, allowing individuals to obtain and reuse their personal data for their own purposes across different services (Right to data portability);
- object to the processing of their personal data (Right to object);
- be informed about any automated decision-making activity (including profiling);
- complain to the appropriate supervisory body eg. the Information Commissioners Office; and
- withdraw consent to personal data being processed (where consent is being relied upon by SLC).

2.7.2 Further information on these rights (including how to exercise these rights), is available to view via Data Subject Rights.

3 Changes to Personal Data

3.1 Accuracy of Personal Data

3.1.1 SLC is required to maintain accurate records of the personal data it processes. The accuracy of personal data is checked at regular intervals, and it is in your interest to keep your personal data up to date eg. by updating your address when you have moved.

3.2 Changes to Personal Data

3.2.1 To assist SLC with its obligation to maintain accurate records, if a data subject's personal data changes, then this can be updated through one of the following channels:

- a customer can confirm/update their personal data using the self-serve online portal. If they are unable to access this portal, then they can contact the appropriate support team using Contact SLC via SLC Home Page/Gov.UK;
- an employee can update their personal data using the internal employee system.
- a contractor can't update their personal data using the internal employee system, so they should contact the People department or their agency directly;
- a supplier should contact their relevant business contact within SLC; and
- Data subjects who do not fall within one of the aforementioned categories, should visit the SLC website and choose their most appropriate contact channel.

4 Data Sharing

4.1 Sharing and Transferring of Personal Data

4.1.1 We may need to share personal data with some third parties, including our service providers. When this occurs, SLC require third parties to respect the security of that data and to treat it in accordance with Data Protection Legislation.

4.1.2 SLC will only transfer personal data outside of the European Economic Area ("EEA") in limited circumstances. When this occurs, SLC will ensure that adequate technical and organisational safeguards are in place, so that any personal data transferred remains secure and is protected.

5 Data Subject Access Requests ("DSARs")

5.1 Contact Points for DSARs

5.1.1 Individuals that SLC holds personal data about have the right to request a copy of their data by phone, online eg. social media or in writing.

5.1.2 Customers or individuals who are not SLC employees can submit a request using the Customer or Sponsor DSAR form, and send to the address or email below:

Data Subject Access Requests
Verification Operations
Student Loans Company Limited

10 Clyde Place
Glasgow
G5 8DF

Email: dsr_slc@slc.co.uk

5.1.3 Employees/Former Employees can submit a request using the Employee DSAR form available on the SLC intranet (accessible to SLC employees only) or contact People_DSAR_Team@SLC.co.uk

6 Security Breaches

6.1 Notification of Security Breaches

6.1.1 A security breach (which may also be referred to as a personal data breach) is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.1.2 If you become aware of a security breach or believe an event may constitute a security breach, you should raise this matter immediately by following the standard SLC complaints procedure.

7 Enforcement

7.1 ICO enforcement and Escalation

7.1.1 The ICO has certain enforcement powers provided under Data Protection Legislation and may serve information, reprimands, enforcement or monetary penalty notices on an organisation where it considers Data Protection Legislation has been breached.

7.1.2 Data Subjects have the right to make a complaint to the ICO in relation to SLC's processing of personal data, by writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Emailing: icocasework@ico.org.uk; or

Calling: 0303 1231113

Live Chat: Contact Us | ICO

Raising a Data Breach: UK GDPR data breach reporting (DPA 2018) | ICO

8 Contact Details

For further guidance on this Policy please contact SLC's DP Office at:

Data Protection Office
Student Loans Company Limited
10 Clyde Place
Glasgow
G5 8DF

or email: DPO@slc.co.uk.

9 Related Documents

This document forms an essential part of SLC's overall policy framework and should be read in accordance with all relevant related documents, including:

Document Description
ICO Guidance on UK General Data Protection Regulation
Data Protection Act 2018
UK GDPR

